REMARKS

The Examiner is thanked for the performance of a through search and for considering the references submitted in the Information Disclosure Statement that was filed on March 17, 2004.

Claims 1, 6, 9-10, 13-16, 21, 23, and 26-28 have been amended. Claims 4-5 and 19-20 have been canceled. Claims 29 and 30 have been added. Hence, Claims 1-3, 6-18, and 21-30 are pending in the application.

Each issue raised in the Office Action mailed November 15, 2005 is addressed hereinafter.

I.   ISSUES NOT RELATING TO THE CITED ART

A.   REJECTIONS UNDER 35 U.S.C. § 101

Claims 9-15 have been rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter.

As amended, independent Claim 9 recites a tangible storage medium. Claims 10-15 depend from independent Claim 9 and thus include each and every feature of the independent claim. For these reasons, each of Claims 9-15 is directed to statutory subject matter. Reconsideration and withdrawal of the rejections of Claims 9-15 under 35 U.S.C. § 101 are respectfully requested.

B.   REJECTIONS UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 13-14 and 26-28 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly lacking definiteness.

As amended, each of Claims 13-14 and 26-28 provides for proper antecedent basis and thus overcomes the rejection under 35 U.S.C. § 112, second paragraph. For this reason, reconsideration and withdrawal of the rejections of Claims 13-14 and 26-28 are respectfully requested.

Attorney Docket No.: 50325-0800

II.   ISSUES RELATING TO THE CITED ART

A.   INDEPENDENT CLAIM 1

Claim 1 has been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Proctor,

U.S. Patent No. 6,530,024 (hereinafter "PROCTOR").

Claim 1 comprises the features of:

> ...
> receiving a set of data regarding a user of a network, wherein the set of data is a
> first set of data that is collected over a first duration of time;
> receiving a second set of data that is collected over a second duration of time,
> **wherein the first duration of time is shorter than the second duration
> of time;**
> **assessing a risk level of the user harming the network based on the second set
> of data,** wherein **the second duration of time is sufficient to collect
> historical data regarding past malicious activities of the user;**
> **assessing a current alert level based on the first set of data,** wherein **the first
> duration of time is of a length appropriate for assessing current
> activities of the user;**
> **automatically deciding on a course of action based on at least one of the risk
> level and the current alert level,** wherein the course of action may be
> adverse to the user although the current alert level is insufficient to
> establish whether the user is performing a malicious action;
> .... .

PROCTOR does not teach, describe, or suggest the above features of Claim 1.

The Office Action asserts that in col. 7, lines 15-26, PROCTOR describes collecting a

first set of data over a first duration of time and collecting a second set of data over a second

duration of time, where the first duration of time is shorter than the second duration of time.

This is incorrect.

PROCTOR describes a system with an adaptive feedback mechanism according to which,

when a security breach is detected, one or more security-related procedures can be modified and

the modified procedures can be implemented in the network. (PROCTOR, Abstract; col. 2, lines

51-60.) Specifically, in col. 7, lines 15-26, PROCTOR describes that updated procedures can be

implemented to perform a more thorough audit of users that are involved in the detected security

Attorney Docket No.: 50325-0800

breach. Significantly, however, PROCTOR does not describe or suggest anything regarding the **durations of time** in which a less-thorough audit and a more-thorough audit are to be performed. On the contrary, in PROCTOR any changes in audit procedures are performed **in response to** detecting the attempt or the occurrence of a security breach. Thus, in the PROCTOR system the duration of time for performing a particular type of audit is governed by the occurrence of a particular event and is NOT guaranteed to be of any particular length. In contrast, Claim 1 recites that the first duration of time in which first data is collected is shorter than a second duration of time in which second data is collected. Further, in Claim 1 the first duration of time is of a length appropriate for assessing the **current activities of the user**, and the second duration of time is sufficient to collect historical data regarding **past malicious activities of the user**.

Claim 1 also comprises the features of assessing a current alert level associated with the current activities of a user based on a first set of data collected over a first duration of time, and assessing a risk level of the user harming the network based on a second set of data collected over a second duration of time. PROCTOR does not teach or describe any of these features.

In col. 6, line 49 to col. 7, line 26, PROCTOR teaches that more thorough audit data is collected in response to detecting that data in event log files indicates a security breach was attempted or has occurred. Thus, PROCTOR teaches that one set of data (more thorough audit data) may be collected in response to analyzing another set of data (data in event logs).

In contrast, in Claim 1 a first set of data is collected over a first duration of time, which is of a length appropriate for assessing the current activities of a user. Based on the first set of data, a current alert level is assessed. A second set of data is collected over a second duration of time, which is sufficient to collect historical data regarding past malicious activities of the user. Based on the second data, a risk level of the user harming the network is assessed. The second set of

13

data, however, is not collected in response to analyzing the first set of data. Thus, nothing in PROCTOR can possibly describe or suggest these features of Claim 1.

Claim 1 also comprises the feature of automatically deciding on a course of action based on at least one of the risk level and the current alert level, wherein the course of action may be adverse to the user although the current alert level is insufficient to establish whether the user is performing a malicious action. There is absolutely nothing in PROCTOR that describes or suggests this feature of Claim 1.

For example, PROCTOR does not describe or suggest assessing a risk level of a user harming the network and assessing a current alert level that reflects the current activities of the user. For this reason, PROCTOR cannot possibly describe or suggest automatically deciding on a course of action based on a risk level and/or a current alert level associated with the user. Further, as discussed above, in the PROCTOR system data collected in event log files is analyzed to determine whether any security breaches were attempted or have occurred; if the data analysis determines that a security breach was attempted or has occurred, then a security response action may be taken. (PROCTOR, col. 6, line 49 to col. 7, line 1.) Thus, the PROCTOR system determines a security response action based on detecting the occurrence of a security breach, and not on any risk levels or alert levels that are assessed for a user as featured in Claim 1.

For the foregoing reasons, PROCTOR does not teach all of the features of Claim 1. Therefore, Claim 1 is patentable under 35 U.S.C. § 102(e) over PROCTOR. Reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

B.   INDEPENDENT CLAIM 16 AND NEW CLAIM 29

Independent Claim 16 has been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PROCTOR.

Attorney Docket No.: 50325-0800

Claim 16 and new Claim 29 include features similar to the features of Claim 1 discussed above, except in the context of a method and an apparatus. Thus, Claims 16 and 29 are patentable under 35 U.S.C. § 102(e) over PROCTOR for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejection of Claim 16, and allowance of Claim 29, are respectfully requested.

C.   DEPENDENT CLAIMS 2-3, 6-8, 17-18, AND 21-22

Claims 2-3, 6-8, 17-18, and 21-22 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PROCTOR.

Each of Claims 2-3, 6-8, 17-18, and 21-22 depends from one of independent Claims 1 and 16, and therefore includes each and every feature of the corresponding independent claim. Thus, each of Claims 2-3, 6-8, 17-18, and 21-22 is allowable for the reasons given above for Claims 1 and 16. In addition, each of Claims 2-3, 6-8, 17-18, and 21-22 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 2-3, 6-8, 17-18, and 21-22 are allowable for the reasons given above with respect to Claims 1 and 16. Reconsideration and withdrawal of the rejections of Claims 2-3, 6-8, 17-18, and 21-22 are respectfully requested.

D.   INDEPENDENT CLAIM 9

Claim 9 has been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PROCTOR.

Claim 9 comprises the features of:

...
receiving signals carrying **network performance information regarding health of a network** and **resource performance information regarding health of resources used by the network;**

15

**assessing a health level based on the network performance information and
the resource performance information;**

... .

PROCTOR does not teach, describe, or suggest the above features of Claim 9. The Office

Action asserts that PROCTOR describes these features of Claim 9 in Figs. 10, 11, and 13, in col.

1, line 65 to col. 2, line 5, and in col. 5, line 61 to col. 7, line 40. This assertion is incorrect.

The Office Action does not specify exactly what in PROCTOR corresponds to or

constitutes the above features of Claim 9. In an Office Action "the particular part relied on must

be designated as nearly as practicable ... The pertinence of each reference, if not apparent, must

be clearly explained ..." (MPEP §707, citing 37 C.F.R. §1.104(c)(2)), and "the particular

figure(s) of the drawings(s), and/or page(s) or paragraph(s) of the reference(s), and/or any

relevant comments briefly stated should be included." (MPEP §707). The present citations to

PROCTOR do not provide the Applicants with adequate notice or reasonable particularity with

respect to the basis of the rejection of Claim 9. Instead, a large portion of PROCTOR (e.g. col.

5, line 61 to col. 7, line 40) is simply identified in a non-specific way. As a result, the Applicants

have had to engage in guesswork to determine the basis of the rejection. The Applicants do not

see any structure or functions in PROCTOR that correspond to the above features of Claim 9.

Specifically, PROCTOR does not describe or suggest anything that corresponds to the

features of Claim 9 of network performance information regarding health of a network, resource

performance information regarding health of resources used by the network, and assessing a

health level based on the network performance information and the resource performance

information.

For example, in Fig. 10 PROCTOR depicts a process for implementing and updating

policies in a computing environment. (PROCTOR, col. 4, lines 20-22.) PROCTOR depicts steps

for creating event log files, collecting records from the event log, performing security analyses

16

Attorney Docket No.: 50325-0800

based on the collected records, and updating some security procedures. (Fig. 10; col. 11, lines 18-48.) However, nothing in Fig. 10 or anything else in PROCTOR describes or suggests **assessing a health level** based on **network performance information** and **resource performance information** as featured in Claim 9.

Similarly, in Fig. 11 PROCTOR depicts a process for updating security procedures based on the identity of a user or users that were involved in a security breach. (See also PROCTOR, col. 11, line 54 to col. 12, line 31.) The security procedures are updated based on the identity of a user or group of users, where such user or group of users are identified in audit information. (PROCTOR, col. 11, lines 56-61.) Such user-identifying audit information, however, is not equivalent to network performance information and resource performance information as featured in Claim 9 because user-identifying information has nothing to do with a network or resources used by the network.

In Fig. 13, PROCTOR depicts a block diagram illustrating the architecture of a security system. Nothing in Fig. 13 is even remotely related to the network performance information and resource performance information featured in Claim 9. Similarly, in col. 1, line 65 to col. 2, line 5, PROCTOR states that a system and method are provided for enhancing security features in a networked computing environment. The system and method provide for creating and implementing one or more security procedures that include audit policies, collection policies, detection policies, and security policies. Significantly, however, there is absolutely nothing in this passage in PROCTOR that describes or suggests anything that is equivalent to the network performance information and resource performance information featured in Claim 9.

Finally, with respect to col. 5, line 61 to col. 7, line 40 in PROCTOR, the Office Action does not identify what exactly it considers as equivalent to the features of Claim 9 of network performance information regarding the health of the network and resource performance

17

information regarding health of resources used by the network. This passage of PROCTOR is not related to any of the above features of Claim 9 and fails to suggest that a health level of the network may be assessed. In contrast, Claim 9 includes the feature of assessing a health level based on the network performance information and the resource performance information.

For the foregoing reasons, PROCTOR does not teach all of the features of Claim 9. Therefore, Claim 9 is patentable under 35 U.S.C. § 102(e) over PROCTOR. Reconsideration and withdrawal of the rejection of Claim 9 are respectfully requested.

E.   INDEPENDENT CLAIM 23 AND NEW CLAIM 30

Independent Claim 23 has been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PROCTOR.

Claim 23 and new Claim 30 include features similar to the features of Claim 9 discussed above, except in the context of a method and an apparatus. Thus, Claims 23 and 30 are patentable under 35 U.S.C. § 102(e) over PROCTOR for at least the reasons given above with respect to Claim 9. Reconsideration and withdrawal of the rejection of Claim 23, and allowance of Claim 30, are respectfully requested.

F.   DEPENDENT CLAIMS 10-12, 15, AND 24-25

Claims 10-12, 15, and 24-25 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by PROCTOR.

Each of Claims 10-12, 15, and 24-25 depends from one of independent Claims 9 and 23, and therefore includes each and every feature of the corresponding independent claim. Thus, each of Claims 10-12, 15, and 24-25 is allowable for the reasons given above for Claims 9 and 23. In addition, each of Claims 10-12, 15, and 24-25 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features

Attorney Docket No.: 50325-0800

is not included at this time. Therefore, it is respectfully submitted that Claims 10-12, 15, and 24-25 are allowable for the reasons given above with respect to Claims 9 and 23. Reconsideration and withdrawal of the rejections of Claims 10-12, 15, and 24-25 are respectfully requested.
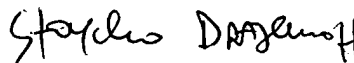
III. CONCLUSION

The Applicants believe that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicants respectfully submit that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the amendments and remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firms check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: February 15, 2006

Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076

19

Attorney Docket No.: 50325-0800